PATENT APPLICATION
Attorney Docket: 10003417-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF APPEALS

Applicant:	Engel
Serial No.:	10/005,749
Filed:	11/7/2001
For:	Secure Communication Protocol Utilizing a Private Key Delivered via a Secure Protocol
Group Art Unit:	2132
Examiner:	Perungavoor, V.

BRIEF FOR APPELLANT

Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the decision of the Examiner dated 5/16/2006, in which the Examiner rejected Claims 1-8 in the above-identified patent application for a third time. After the previous rejection of the claims, Applicant filed an appeal including the arguments made in traversing the original rejection of the claims. The Examiner, after reconsideration of those arguments, abandoned the Examiner's first grounds for rejection, reopened prosecution in this patent application, and presented a new grounds for rejection. Applicant believes that the new grounds for rejection are also flawed and commenced this new appeal to address the new grounds for rejection.

I. REAL PARTY IN INTEREST

The real party in interest is Agilent Technologies, Inc. having an address as shown below.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to appellant, the appellant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

III. STATUS OF THE CLAIMS

Claims 1-8 are currently pending in the above-identified patent application. In the Office Action dated 2/06/2006, the Examiner rejected Claims 1-8 and indicated that the Action was final.

IV. STATUS OF AMENDMENTS

No amendments have been filed since the final rejection.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Refer to Figure 1 and the discussion thereof that begins on page 3, at line 15 of the specification. The present invention is directed to computer networks in which a computer having limited computational resources (node 12) wishes to communicate with another computer (server 14) over an insecure network (network 17) using an encryption protocol that requires a key. The computationally limited computer receives the key with the help of a third computer (workstation 21) having more computational capacity and that utilizes a secure communication protocol to obtain the key from server 14.

With reference to Claim 1, the present invention is a method for operating a computer system having first, second, and third data processors connected by a network that includes network 13, and network 17 which is an insecure network. The first processor corresponds to node 12, and the second processor corresponds to server 14. The third processor is workstation 21. The second data processor (server 14) sends a key for a first encryption protocol to the third data processor (workstation 21) using a second encryption protocol. The third data processor (workstation 21) then forwards the key to the first data processor (node 12). The first data processor (node 12) then uses the key to send a message to the second data processor (server 14) using the key, the message being encrypted in the first encryption

protocol. With reference to Claim 4, the process is initiated in response to a message from the first data processor to the second data processor.

With reference to Claim 2, node 12 has insufficient computational resources to execute the second encryption protocol used by server 14 to send the key to workstation 21. With reference to Claim 3, the second encryption protocol is a public key encryption protocol. With reference to Claim 5, network segment 17 is the internet. With reference to Claim 6, network segment 13 includes a local area network. With reference to Claim 7, the local area network is more secure than network 17. With reference to Claim 8, the first encryption protocol requires less computational resources than the second encryption protocol.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Rejection of Claims 1-8 under 35 U.S.C. 102(b) as being anticipated by US Patent 5,784,463 to Chen, et al. ("Chen")

VII. ARGUMENT

A. The Examiner's Burden under 35 U.S.C. 102

The Examiner has the burden of showing by reference to the cited art each claim limitation in the reference. Anticipation under 35 U.S.C. 102 requires that each element of the claim in issue be found either expressly or inherently in a single prior art reference. In re King, 231 USPQ 136, 138 (Fed. Cir. 1986); Kalman v. Kimberly-Clark Corp., 218 USPQ 781, 789 (Fed. Cir. 1983). The mere fact that a certain thing may result from a given set of circumstances is not sufficient to sustain a rejection for anticipation. *Ex parte Skinner*, 2 USPQ2d 1788, 1789 (BdPatApp&Int 1986). "When the PTO asserts that there is an explicit or implicit teaching or suggestion in the prior art, it must indicate where such a teaching or suggestion appears in the reference" (*In re* Rijckaert, 28 USPQ2d, 1955, 1957).

Under the doctrine of inherency, if an element is not expressly disclosed in a prior art reference, the reference will still be deemed to anticipate a subsequent claim if the missing element "is necessarily present in the thing described in the reference " Cont'l Can Co. v. Monsanto Co., 948 F.2d 1264, 1268, 20 USPQ2d 1746, 1749(Fed. Cir. 1991). "Inherent anticipation requires that the missing descriptive material is 'necessarily present,' not merely probably or possibly present, in the prior art." *Trintec Indus., Inc. v. Top-U.S.A. Corp.*, 295

F.3d 1292, 1295, 63 USPQ2d 1597, 1599 (Fed. Cir. 2002) (quoting *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999)).

B. Rejection of Claims 1 and 3

Claim 1 deals with a communication protocol between three data processors on a network in which the second and third data processors are connected by an insecure network segment. Refer to Figure 1 of the present application. Two encryption protocols are used during the communication. In the first step of the protocol, the second data processor (server 14) sends a message to the third data processor (workstation 21) containing an encryption key for a first encryption protocol. This message is sent using a second encryption protocol. The third data processor (workstation 21) then sends that key to the first data processor (node 12). The first data processor (node 12) then sends a message to the second data processor (server 14) using that key.

The Examiner looks to Figure 3A of Chen as teaching the method of Claim 1. Figure 3A is a flow chart of the method taught in Chen. In particular, the Examiner looks to the step labeled 60 as corresponding to causing the second data processor to send an encryption key for a first encryption protocol to the third data processor using a second encryption protocol.

Refer to column 14 of Chen starting at line 40. Chen teaches that step 60 corresponds to a token issuer or certification authority distributing a token having a public key (Pi) to the user, i.e., client 10 shown in Figures 1 and 2. Hence, the token issuer (or certification authority) must correspond to the second data processor, and the user must correspond to the third data processor. It should be noted that Chen does not teach that this transmission is encrypted using any encryption protocol. Furthermore, since the step involves transmitting a public key, no encryption is needed. Hence, Applicant submits that the teaching identified by the Examiner does not satisfy the first limitation of Claim 1.

The Examiner goes on to identify item 70 in Figure 3A as corresponding to the claim limitation "causing said third data processor to forward said encryption key to said first data processor". Referring again to the passage cited above from Chen, item 70 refers to the token issuer sending the server private key, Pr, and signed server public key certificates to the authentication server. Since the token issuer is the second data processor and the client is the

third data processor, the authentication server must be the first data processor recited in Claim 1. However, the claim limitation in question requires a message from the third data processor to the first data processor and the message must include the key sent to the third data processor in the first step.

Hence, the step at item 70 fails to meet the second limitation of Claim 1 for two reasons. First, the transmission is from the second data processor to the first data processor. Second, the key (Pi) is not sent in this transmission. Chen only teaches sending public key certificates. While the certificates cannot be verified without knowledge of Pi, one cannot deduce Pi from the certificates. Hence, the passage step cited by the Examiner fails to satisfy the second limitation of Claim 1.

The Examiner goes on to identify item 90 as corresponding to the claim limitation "causing said first data processor to send a message to said second data processor utilizing said encryption key and said first encryption protocol, said message being sent over a communication path comprising said insecure network segment". Referring again to the above-identified passage in Chen, Chen teaches that the server, i.e., the first data processor of Claim 1, sends the public key certificate it received from the token issuer, i.e., the second data processor, to the user, i.e., the third data processor. That is, the message is sent from the first data processor to the third data processor, not from the first data processor to the second data processor.

Finally, it should be noted that in the scheme taught in Chen depends on the authentication server never knowing the first key Pi. Hence, the method taught therein depends on the third data processor never sending the first key to the authentication processor.

Hence, the method identified by the Examiner fails to satisfy all three of the limitations of Claim 1. In addition, the method taught in Chen would not function properly if the second limitation of Claim 1 were satisfied. Accordingly, Claim 1 and the claims dependent therefrom are not anticipated by Chen.

C. Rejection of Claim 2

In addition to the limitations of Claim 1, Claim 2 requires that the first data processor have insufficient computational resources to execute the second encryption protocol. The Examiner maintains that Chen teaches this limitation and cites Figure 1b item 10 and col. 1, lines 41-49 as supporting this assertion.

First, item 10 shown in Figure 1B is the client computer. As noted above, these data processors must correspond to the third data processor recited in the claim. As noted above, the second encryption protocol must correspond to the public key protocol that uses the public key Pi, since this is the key that is sent to the client computers. Since the client computers use this key to verify the certificates sent from the authentication server, the client computers must have the computational resources to execute the public key encryption scheme, i.e., the second encryption protocol. Hence, the Examiner's argument is flawed in two aspects: the data processor identified is the wrong data processor, and that data processor does have the computational resources in question.

As noted above, the first data processor must correspond to the authentication server 20. Chen also teaches that this server performs public key decryption. Hencc, this server also has sufficient computational resources to perform the second encryption protocol. Hence, there are additional grounds for allowing Claim 2.

D. Rejection of Claim 4

In addition to the limitations of Claim 1, Claim 4 requires that the step of causing the second data processor to send an encryption key to the third data processor is initiated in response to a message from the first data processor to the second data processor. The Examiner states that Chen discloses that the second processor sends a message and key to the first data processor, and cites item 35 in Figure 1A as supporting this assertion.

Item 35 in Figure 1A is the token issuer, i.e., the second data processor of Claim 1. The issue is not whether a message is sent from the token issuer to third data processor containing the encryption key, but rather thc event that triggers the transmission. As noted above, the Examiner inherently argues that the authentication server is the first data processor

of Claim 1, the client is the third data processor, and the token issuer is the third data processor. Claim 4 requires that the token issuer sends the public key to the client in response to a message from the authentication server.

Applicant can find no teaching in Chen with respect to the event that causes the distribution of the public key encryptions keys to the clients. Furthermore, Chen teaches that token issuer sends the certificates and keys to the authentication server at the same time or after the token server sends the key to the client. Hence, it would appear that the key is sent in response to a message from some other entity or part of the internal workings of the token server. Accordingly, Applicant submits the Examiner has not satisfied the Examiner's burden of proof with respect to the rejection of Claim 4, and hence, there are additional grounds for allowing Claim 4.

E. Rejection of Claim 5

In addition to the limitations of Claim 1, Claim 5 requires that the network segment connecting the second and third data processors comprises the internet. The Examiner points to item 5 as comprising the internet in support of the Examiner's assertion that Chen teaches the additional limitation of Claim 5.

As noted above, the second and third data processors identified by the Examiner are the token issuer and the client computer. These computers communicate directly with each other in the scheme shown in Chen. They do not use network 5 identified by the Examiner. Accordingly, there are additional grounds for allowing Claim 5.

F. Rejection of Claim 6

In addition to the limitations of Claim 1, Claim 6 requires that the network segment connecting the first and third data processors comprises a local area network. The Examiner points to the passage at col. 1, lines 50-59 of Chen as teaching this limitation. Once again, Applicant must disagree.

The first and third data processors correspond to the authentication server and the client computer, respectively. These computers communicate with each other over the internet in the scheme shown in Chen.

Furthermore, the passage identified by the Examiner does not refer to any local area network. The passage does mention a firewall. However, firewalls are often implemented on the computer to be protected, and hence, do not require a local area network. Hence, there are additional grounds for allowing Claim 6.

G. Rejection of Claim 7

In addition to the limitations of Claim 1, Claim 7 requires that the network segment connecting the first and third data processors has a higher level of security than the network segment connecting the second and third data processors. The Examiner points to the passage at col. 2, lines 8-18 as teaching this limitation. Once again, Applicant must disagree. The cited passage does not refer to the relative security of the network segments. The passage relates to the increased security provided by the scheme taught in Chen.

As noted above, the first and third data processors of Claim 1 must correspond to the authentication server and client computers, respectively, in the scheme taught in Chen. As noted above, these computers communicate over the internet, the lowest security network segment. The second and third data processors, i.e., the token issuer and client computer, respectively, communicate directly in the scheme taught in Chen. This is the segment having the highest security. Hence, if anytbing, Chen teaches away from the limitation of Claim 7. Hence, there are additional grounds for allowing Claim 7.

H. Rejection of Claim 8

In addition to the limitations of Claim 1, Claim 8 requires that the first encryption protocol require less computational resources than the second encryption protocol. The Examiner points to the same passages indicated in the Examiner's rejection of Claim 2 discussed above. This passage does not teach anything with respect to the existence or the nature of the first encryption protocol,

As noted above, Chen teaches that the token issuer provide a public key to the client in a message sent from the token issuer to the client. The first encryption protocol of Claim 1 is the protocol used to send this message. However, Chen is silent as to whether or not this message is encrypted. Hence, the Examiner has not satisfied the Examiner's burden of

showing that this message must have been encrypted with a protocol requiring less computational resources than the public key protocol. Accordingly, there are additional grounds for allowing Claim 8.

VII. CONCLUSION

Appellants respectfully submit that for the reasons of fact and law argued herein, the decision of the Examiner in finally rejecting Claims 1-8 should be reversed.

I hereby certify that this paper (along with any others attached hereto) is being sent via facsimile to fax number: 571-273-8300

Respectfully Submitted,

Calvin B. Ward
Registration No. 30,896
Date: July 24, 2006

Agilent Technologies, Inc.
Legal Department, M/S DL429
Intellectual Property Administration
P.O. Box 7599
Loveland, CO 80537-0599
Telephone (925) 855-0413
Telefax (925)855-9214

APPENDIX

THE CLAIMS ON APPEAL:

1. A method for operating a computer system having first, second, and third data processors connected by a network wherein said second and third data processors are connected by an insecure network segment, said method comprising the steps of:

causing said second data processor to send an encryption key for a first encryption protocol to said third data processor utilizing a second encryption protocol;

causing said third data processor to forward said encryption key to said first data processor; and

causing said first data processor to send a message to said second data processor utilizing said encryption key and said first encryption protocol, said message being sent over a communication path comprising said insecure network segment.

2. The method of Claim 1 wherein said first data processor has insufficient computational resources to execute said second encryption protocol.

3. The method of Claim 1 wherein said second encryption protocol is a public key encryption protocol.

4. The method of Claim 1 wherein said step of causing said second data processor to send an encryption key is initiated in response to a message from said first data processor to said second data processor.

5. The method of Claim 1 wherein said insecure network segment comprises the Internet.

6. The method of Claim 1 wherein said network segment connecting said first and third data processors comprises a local area network.

7. The method of Claim 1 wherein said first and third data processors are connected by a network segment that has a higher level of security than said insecure network segment.

8. The method of Claim 1 wherein said first encryption protocol requires less computational resources than said second encryption protocol

Evidence Appendix

none

Related Proceedings Appendix

none

PATENT APPLICATION
Attorney Docket: 10003417-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS

Applicant:	Engel
Serial No.:	10/005,749
Filed:	11/7/2001
For:	Secure Communication Protocol Utilizing a Private Key Delivered via a Secure Protocol
Group Art Unit:	2132
Examiner:	Perungavoor, V.

BRIEF FOR APPELLANT

Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the decision of the Examiner dated 5/16/2006, in which the Examiner rejected Claims 1-8 in the above-identified patent application for a third time. After the previous rejection of the claims, Applicant filed an appeal including the arguments made in traversing the original rejection of the claims. The Examiner, after reconsideration of those arguments, abandoned the Examiner's first grounds for rejection, reopened prosecution in this patent application, and presented a new grounds for rejection. Applicant believes that the new grounds for rejection are also flawed and commenced this new appeal to address the new grounds for rejection.

I. REAL PARTY IN INTEREST

The real party in interest is Agilent Technologies, Inc. having an address as shown below.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to appellant, the appellant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

III. STATUS OF THE CLAIMS

Claims 1-8 are currently pending in the above-identified patent application. In the Office Action dated 2/06/2006, the Examiner rejected Claims 1-8 and indicated that the Action was final.

IV. STATUS OF AMENDMENTS

No amendments have been filed since the final rejection.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Refer to Figure 1 and the discussion thereof that begins on page 3, at line 15 of the specification. The present invention is directed to computer networks in which a computer having limited computational resources (node 12) wishes to communicate with another computer (server 14) over an insecure network (network 17) using an encryption protocol that requires a key. The computationally limited computer receives the key with the help of a third computer (workstation 21) having more computational capacity and that utilizes a secure communication protocol to obtain the key from server 14.

With reference to Claim 1, the present invention is a method for operating a computer system having first, second, and third data processors connected by a network that includes network 13, and network 17 which is an insecure network. The first processor corresponds to node 12, and the second processor corresponds to server 14. The third processor is workstation 21. The second data processor (server 14) sends a key for a first encryption protocol to the third data processor (workstation 21) using a second encryption protocol. The third data processor (workstation 21) then forwards the key to the first data processor (node 12). The first data processor (node 12) then uses the key to send a message to the second data processor (server 14) using the key, the message being encrypted in the first encryption

protocol. With reference to Claim 4, the process is initiated in response to a message from the first data processor to the second data processor.

With reference to Claim 2, node 12 has insufficient computational resources to execute the second encryption protocol used by server 14 to send the key to workstation 21. With reference to Claim 3, the second encryption protocol is a public key encryption protocol. With reference to Claim 5, network segment 17 is the internet. With reference to Claim 6, network segment 13 includes a local area network. With reference to Claim 7, the local area network is more secure than network 17. With reference to Claim 8, the first encryption protocol requires less computational resources than the second encryption protocol.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Rejection of Claims 1-8 under 35 U.S.C. 102(b) as being anticipated by US Patent 5,784,463 to Chen, et al. ("Chen")

VII. ARGUMENT

A. The Examiner's Burden under 35 U.S.C. 102

The Examiner has the burden of showing by reference to the cited art each claim limitation in the reference. Anticipation under 35 U.S.C. 102 requires that each element of the claim in issue be found either expressly or inherently in a single prior art reference. In re King, 231 USPQ 136, 138 (Fed. Cir. 1986); Kalman v. Kimberly-Clark Corp., 218 USPQ 781, 789 (Fed. Cir. 1983). The mere fact that a certain thing may result from a given set of circumstances is not sufficient to sustain a rejection for anticipation. *Ex parte Skinner*, 2 USPQ2d 1788, 1789 (BdPatApp&Int 1986). "When the PTO asserts that there is an explicit or implicit teaching or suggestion in the prior art, it must indicate where such a teaching or suggestion appears in the reference" (*In re* Rijckaert, 28 USPQ2d, 1955, 1957).

Under the doctrine of inherency, if an element is not expressly disclosed in a prior art reference, the reference will still be deemed to anticipate a subsequent claim if the missing element "is necessarily present in the thing described in the reference " Cont'l Can Co. v. Monsanto Co., 948 F.2d 1264, 1268, 20 USPQ2d 1746, 1749(Fed. Cir. 1991). "Inherent anticipation requires that the missing descriptive material is 'necessarily present,' not merely probably or possibly present, in the prior art." *Trintec Indus., Inc. v. Top-U.S.A. Corp.*, 295

F.3d 1292, 1295, 63 USPQ2d 1597, 1599 (Fed. Cir. 2002) (quoting *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999)).

B. Rejection of Claims 1 and 3

Claim 1 deals with a communication protocol between three data processors on a network in which the second and third data processors are connected by an insecure network segment. Refer to Figure 1 of the present application. Two encryption protocols are used during the communication. In the first step of the protocol, the second data processor (server 14) sends a message to the third data processor (workstation 21) containing an encryption key for a first encryption protocol. This message is sent using a second encryption protocol. The third data processor (workstation 21) then sends that key to the first data processor (node 12). The first data processor (node 12) then sends a message to the second data processor (server 14) using that key.

The Examiner looks to Figure 3A of Chen as teaching the method of Claim 1. Figure 3A is a flow chart of the method taught in Chen. In particular, the Examiner looks to the step labeled 60 as corresponding to causing the second data processor to send an encryption key for a first encryption protocol to the third data processor using a second encryption protocol.

Refer to column 14 of Chen starting at line 40. Chen teaches that step 60 corresponds to a token issuer or certification authority distributing a token having a public key (Pi) to the user, i.e., client 10 shown in Figures 1 and 2. Hence, the token issuer (or certification authority) must correspond to the second data processor, and the user must correspond to the third data processor. It should be noted that Chen does not teach that this transmission is encrypted using any encryption protocol. Furthermore, since the step involves transmitting a public key, no encryption is needed. Hence, Applicant submits that the teaching identified by the Examiner does not satisfy the first limitation of Claim 1.

The Examiner goes on to identify item 70 in Figure 3A as corresponding to the claim limitation "causing said third data processor to forward said encryption key to said first data processor". Referring again to the passage cited above from Chen, item 70 refers to the token issuer sending the server private key, Pr, and signed server public key certificates to the authentication server. Since the token issuer is the second data processor and the client is the

third data processor, the authentication server must be the first data processor recited in Claim 1. However, the claim limitation in question requires a message from the third data processor to the first data processor and the message must include the key sent to the third data processor in the first step.

Hence, the step at item 70 fails to meet the second limitation of Claim 1 for two reasons. First, the transmission is from the second data processor to the first data processor. Second, the key (Pi) is not sent in this transmission. Chen only teaches sending public key certificates. While the certificates cannot be verified without knowledge of Pi, one cannot deduce Pi from the certificates. Hence, the passage step cited by the Examiner fails to satisfy the second limitation of Claim 1.

The Examiner goes on to identify item 90 as corresponding to the claim limitation "causing said first data processor to send a message to said second data processor utilizing said encryption key and said first encryption protocol, said message being sent over a communication path comprising said insecure network segment". Referring again to the above-identified passage in Chen, Chen teaches that the server, i.e., the first data processor of Claim 1, sends the public key certificate it received from the token issuer, i.e., the second data processor, to the user, i.e., the third data processor. That is, the message is sent from the first data processor to the third data processor, not from the first data processor to the second data processor.

Finally, it should be noted that in the scheme taught in Chen depends on the authentication server never knowing the first key Pi. Hence, the method taught therein depends on the third data processor never sending the first key to the authentication processor.

Hence, the method identified by the Examiner fails to satisfy all three of the limitations of Claim 1. In addition, the method taught in Chen would not function properly if the second limitation of Claim 1 were satisfied. Accordingly, Claim 1 and the claims dependent therefrom are not anticipated by Chen.

C. Rejection of Claim 2

In addition to the limitations of Claim 1, Claim 2 requires that the first data processor have insufficient computational resources to execute the second encryption protocol. The Examiner maintains that Chen teaches this limitation and cites Figure 1b item 10 and col. 1, lines 41-49 as supporting this assertion.

First, item 10 shown in Figure 1B is the client computer. As noted above, these data processors must correspond to the third data processor recited in the claim. As noted above, the second encryption protocol must correspond to the public key protocol that uses the public key Pi, since this is the key that is sent to the client computers. Since the client computers use this key to verify the certificates sent from the authentication server, the client computers must have the computational resources to execute the public key encryption scheme, i.e., the second encryption protocol. Hence, the Examiner's argument is flawed in two aspects: the data processor identified is the wrong data processor, and that data processor does have the computational resources in question.

As noted above, the first data processor must correspond to the authentication server 20. Chen also teaches that this server performs public key decryption. Hence, this server also has sufficient computational resources to perform the second encryption protocol. Hence, there are additional grounds for allowing Claim 2.

D. Rejection of Claim 4

In addition to the limitations of Claim 1, Claim 4 requires that the step of causing the second data processor to send an encryption key to the third data processor is initiated in response to a message from the first data processor to the second data processor. The Examiner states that Chen discloses that the second processor sends a message and key to the first data processor, and cites item 35 in Figure 1A as supporting this assertion.

Item 35 in Figure 1A is the token issuer, i.e., the second data processor of Claim 1. The issue is not whether a message is sent from the token issuer to third data processor containing the encryption key, but rather the event that triggers the transmission. As noted above, the Examiner inherently argues that the authentication server is the first data processor

of Claim 1, the client is the third data processor, and the token issuer is the third data processor. Claim 4 requires that the token issuer sends the public key to the client in response to a message from the authentication server.

Applicant can find no teaching in Chen with respect to the event that causes the distribution of the public key encryptions keys to the clients. Furthermore, Chen teaches that token issuer sends the certificates and keys to the authentication server at the same time or after the token server sends the key to the client. Hence, it would appear that the key is sent in response to a message from some other entity or part of the internal workings of the token server. Accordingly, Applicant submits the Examiner has not satisfied the Examiner's burden of proof with respect to the rejection of Claim 4, and hence, there are additional grounds for allowing Claim 4.

E. Rejection of Claim 5

In addition to the limitations of Claim 1, Claim 5 requires that the network segment connecting the second and third data processors comprises the internet. The Examiner points to item 5 as comprising the internet in support of the Examiner's assertion that Chen teaches the additional limitation of Claim 5.

As noted above, the second and third data processors identified by the Examiner are the token issuer and the client computer. These computers communicate directly with each other in the scheme shown in Chen. They do not use network 5 identified by the Examiner. Accordingly, there are additional grounds for allowing Claim 5.

F. Rejection of Claim 6

In addition to the limitations of Claim 1, Claim 6 requires that the network segment connecting the first and third data processors comprises a local area network. The Examiner points to the passage at col. 1, lines 50-59 of Chen as teaching this limitation. Once again, Applicant must disagree.

The first and third data processors correspond to the authentication server and the client computer, respectively. These computers communicate with each other over the internet in the scheme shown in Chen.

Furthermore, the passage identified by the Examiner does not refer to any local area network. The passage does mention a firewall. However, firewalls are often implemented on the computer to be protected, and hence, do not require a local area network. Hence, there are additional grounds for allowing Claim 6.

G. Rejection of Claim 7

In addition to the limitations of Claim 1, Claim 7 requires that the network segment connecting the first and third data processors has a higher level of security than the network segment connecting the second and third data processors. The Examiner points to the passage at col. 2, lines 8-18 as teaching this limitation. Once again, Applicant must disagree. The cited passage does not refer to the relative security of the network segments. The passage relates to the increased security provided by the scheme taught in Chen.

As noted above, the first and third data processors of Claim 1 must correspond to the authentication server and client computers, respectively, in the scheme taught in Chen. As noted above, these computers communicate over the internet, the lowest security network segment. The second and third data processors, i.e., the token issuer and client computer, respectively, communicate directly in the scheme taught in Chen. This is the segment having the highest security. Hence, if anything, Chen teaches away from the limitation of Claim 7. Hence, there are additional grounds for allowing Claim 7.

H. Rejection of Claim 8

In addition to the limitations of Claim 1, Claim 8 requires that the first encryption protocol require less computational resources than the second encryption protocol. The Examiner points to the same passages indicated in the Examiner's rejection of Claim 2 discussed above. This passage does not teach anything with respect to the existence or the nature of the first encryption protocol,

As noted above, Chen teaches that the token issuer provide a public key to the client in a message sent from the token issuer to the client. The first encryption protocol of Claim 1 is the protocol used to send this message. However, Chen is silent as to whether or not this message is encrypted. Hence, the Examiner has not satisfied the Examiner's burden of

showing that this message must have been encrypted with a protocol requiring less computational resources than the public key protocol. Accordingly, there are additional grounds for allowing Claim 8.

VII. CONCLUSION

Appellants respectfully submit that for the reasons of fact and law argued herein, the decision of the Examiner in finally rejecting Claims 1-8 should be reversed.

I hereby certify that this paper (along with any others attached hereto) is being sent via facsimile to fax number: 571-273-8300

Respectfully Submitted,

Calvin B. Ward
Registration No. 30,896
Date: July 24, 2006

Agilent Technologies, Inc.
Legal Department, M/S DL429
Intellectual Property Administration
P.O. Box 7599
Loveland, CO 80537-0599
Telephone (925) 855-0413
Telefax (925)855-9214

APPENDIX

THE CLAIMS ON APPEAL:

1. A method for operating a computer system having first, second, and third data processors connected by a network wherein said second and third data processors are connected by an insecure network segment, said method comprising the steps of:

causing said second data processor to send an encryption key for a first encryption protocol to said third data processor utilizing a second encryption protocol;

causing said third data processor to forward said encryption key to said first data processor; and

causing said first data processor to send a message to said second data processor utilizing said encryption key and said first encryption protocol, said message being sent over a communication path comprising said insecure network segment.

2. The method of Claim 1 wherein said first data processor has insufficient computational resources to execute said second encryption protocol.

3. The method of Claim 1 wherein said second encryption protocol is a public key encryption protocol.

4. The method of Claim 1 wherein said step of causing said second data processor to send an encryption key is initiated in response to a message from said first data processor to said second data processor.

5. The method of Claim 1 wherein said insecure network segment comprises the Internet.

6. The method of Claim 1 wherein said network segment connecting said first and third data processors comprises a local arca network.

7. The method of Claim 1 wherein said first and third data processors are connected by a network segment that has a higher level of security than said insecure network segment.

8. The method of Claim 1 wherein said first encryption protocol requires less computational resources than said second encryption protocol

Evidence Appendix

none

Related Proceedings Appendix

none

PATENT APPLICATION
Attorney Docket: 10003417-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS

Applicant:	Engel
Serial No.:	10/005,749
Filed:	11/7/2001
For:	Secure Communication Protocol Utilizing a Private Key Delivered via a Secure Protocol
Group Art Unit:	2132
Examiner:	Perungavoor, V.

BRIEF FOR APPELLANT

Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the decision of the Examiner dated 5/16/2006, in which the Examiner rejected Claims 1-8 in the above-identified patent application for a third time. After the previous rejection of the claims, Applicant filed an appeal including the arguments made in traversing the original rejection of the claims. The Examiner, after reconsideration of those arguments, abandoned the Examiner's first grounds for rejection, reopened prosecution in this patent application, and presented a new grounds for rejection. Applicant believes that the new grounds for rejection are also flawed and commenced this new appeal to address the new grounds for rejection.

I. REAL PARTY IN INTEREST

The real party in interest is Agilent Technologies, Inc. having an address as shown below.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to appellant, the appellant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

III. STATUS OF THE CLAIMS

Claims 1-8 are currently pending in the above-identified patent application. In the Office Action dated 2/06/2006, the Examiner rejected Claims 1-8 and indicated that the Action was final.

IV. STATUS OF AMENDMENTS

No amendments have been filed since the final rejection.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Refer to Figure 1 and the discussion thereof that begins on page 3, at line 15 of the specification. The present invention is directed to computer networks in which a computer having limited computational resources (node 12) wishes to communicate with another computer (server 14) over an insecure network (network 17) using an encryption protocol that requires a key. The computationally limited computer receives the key with the help of a third computer (workstation 21) having more computational capacity and that utilizes a secure communication protocol to obtain the key from server 14.

With reference to Claim 1, the present invention is a method for operating a computer system having first, second, and third data processors connected by a network that includes network 13, and network 17 which is an insecure network. The first processor corresponds to node 12, and the second processor corresponds to server 14. The third processor is workstation 21. The second data processor (server 14) sends a key for a first encryption protocol to the third data processor (workstation 21) using a second encryption protocol. The third data processor (workstation 21) then forwards the key to the first data processor (node 12). The first data processor (node 12) then uses the key to send a message to the second data processor (server 14) using the key, the message being encrypted in the first encryption

protocol. With reference to Claim 4, the process is initiated in response to a message from the first data processor to the second data processor.

With reference to Claim 2, node 12 has insufficient computational resources to execute the second encryption protocol used by server 14 to send the key to workstation 21. With reference to Claim 3, the second encryption protocol is a public key encryption protocol. With reference to Claim 5, network segment 17 is the internet. With reference to Claim 6, network segment 13 includes a local area network. With reference to Claim 7, the local area network is more secure than network 17. With reference to Claim 8, the first encryption protocol requires less computational resources than the second encryption protocol.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Rejection of Claims 1-8 under 35 U.S.C. 102(b) as being anticipated by US Patent 5,784,463 to Chen, et al. ("Chen")

VII. ARGUMENT

A. The Examiner's Burden under 35 U.S.C. 102

The Examiner has the burden of showing by reference to the cited art each claim limitation in the reference. Anticipation under 35 U.S.C. 102 requires that each element of the claim in issue be found either expressly or inherently in a single prior art reference. In re King, 231 USPQ 136, 138 (Fed. Cir. 1986); Kalman v. Kimberly-Clark Corp., 218 USPQ 781, 789 (Fed. Cir. 1983). The mere fact that a certain thing may result from a given set of circumstances is not sufficient to sustain a rejection for anticipation. *Ex parte Skinner*, 2 USPQ2d 1788, 1789 (BdPatApp&Int 1986). "When the PTO asserts that there is an explicit or implicit teaching or suggestion in the prior art, it must indicate where such a teaching or suggestion appears in the reference" (*In re* Rijckaert, 28 USPQ2d, 1955, 1957).

Under the doctrine of inherency, if an element is not expressly disclosed in a prior art reference, the reference will still be deemed to anticipate a subsequent claim if the missing element "is necessarily present in the thing described in the reference " Cont'l Can Co. v. Monsanto Co., 948 F.2d 1264, 1268, 20 USPQ2d 1746, 1749(Fed. Cir. 1991). "Inherent anticipation requires that the missing descriptive material is 'necessarily present,' not merely probably or possibly present, in the prior art." *Trintec Indus., Inc. v. Top-U.S.A. Corp.*, 295

F.3d 1292, 1295, 63 USPQ2d 1597, 1599 (Fed. Cir. 2002) (quoting *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999)).

B. Rejection of Claims 1 and 3

Claim 1 deals with a communication protocol between three data processors on a network in which the second and third data processors are connected by an insecure network segment. Refer to Figure 1 of the present application. Two encryption protocols are used during the communication. In the first step of the protocol, the second data processor (server 14) sends a message to the third data processor (workstation 21) containing an encryption key for a first encryption protocol. This message is sent using a second encryption protocol. The third data processor (workstation 21) then sends that key to the first data processor (node 12). The first data processor (node 12) then sends a message to the second data processor (server 14) using that key.

The Examiner looks to Figure 3A of Chen as teaching the method of Claim 1. Figure 3A is a flow chart of the method taught in Chen. In particular, the Examiner looks to the step labeled 60 as corresponding to causing the second data processor to send an encryption key for a first encryption protocol to the third data processor using a second encryption protocol.

Refer to column 14 of Chen starting at line 40. Chen teaches that step 60 corresponds to a token issuer or certification authority distributing a token having a public key (Pi) to the user, i.e., client 10 shown in Figures 1 and 2. Hence, the token issuer (or certification authority) must correspond to the second data processor, and the user must correspond to the third data processor. It should be noted that Chen does not teach that this transmission is encrypted using any encryption protocol. Furthermore, since the step involves transmitting a public key, no encryption is needed. Hence, Applicant submits that the teaching identified by the Examiner does not satisfy the first limitation of Claim 1.

The Examiner goes on to identify item 70 in Figure 3A as corresponding to the claim limitation "causing said third data processor to forward said encryption key to said first data processor". Referring again to the passage cited above from Chen, item 70 refers to the token issuer sending the server private key, Pr, and signed server public key certificates to the authentication server. Since the token issuer is the second data processor and the client is the

third data processor, the authentication server must be the first data processor recited in Claim 1. However, the claim limitation in question requires a message from the third data processor to the first data processor and the message must include the key sent to the third data processor in the first step.

Hence, the step at item 70 fails to meet the second limitation of Claim 1 for two reasons. First, the transmission is from the second data processor to the first data processor. Second, the key (Pi) is not sent in this transmission. Chen only teaches sending public key certificates. While the certificates cannot be verified without knowledge of Pi, one cannot deduce Pi from the certificates. Hence, the passage step cited by the Examiner fails to satisfy the second limitation of Claim 1.

The Examiner goes on to identify item 90 as corresponding to the claim limitation "causing said first data processor to send a message to said second data processor utilizing said encryption key and said first encryption protocol, said message being sent over a communication path comprising said insecure network segment". Referring again to the above-identified passage in Chen, Chen teaches that the server, i.e., the first data processor of Claim 1, sends the public key certificate it received from the token issuer, i.e., the second data processor, to the user, i.e., the third data processor. That is, the message is sent from the first data processor to the third data processor, not from the first data processor to the second data processor.

Finally, it should be noted that in the scheme taught in Chen depends on the authentication server never knowing the first key Pi. Hence, the method taught therein depends on the third data processor never sending the first key to the authentication processor.

Hence, the method identified by the Examiner fails to satisfy all three of the limitations of Claim 1. In addition, the method taught in Chen would not function properly if the second limitation of Claim 1 were satisfied. Accordingly, Claim 1 and the claims dependent therefrom are not anticipated by Chen.

C. Rejection of Claim 2

In addition to the limitations of Claim 1, Claim 2 requires that the first data processor have insufficient computational resources to execute the second encryption protocol. The Examiner maintains that Chen teaches this limitation and cites Figure 1b item 10 and col. 1, lines 41-49 as supporting this assertion.

First, item 10 shown in Figure 1B is the client computer. As noted above, these data processors must correspond to the third data processor recited in the claim. As noted above, the second encryption protocol must correspond to the public key protocol that uses the public key Pi, since this is the key that is sent to the client computers. Since the client computers use this key to verify the certificates sent from the authentication server, the client computers must have the computational resources to execute the public key encryption scheme, i.e., the second encryption protocol. Hence, the Examiner's argument is flawed in two aspects: the data processor identified is the wrong data processor, and that data processor does have the computational resources in question.

As noted above, the first data processor must correspond to the authentication server 20. Chen also teaches that this server performs public key decryption. Hence, this server also has sufficient computational resources to perform the second encryption protocol. Hence, there are additional grounds for allowing Claim 2.

D. Rejection of Claim 4

In addition to the limitations of Claim 1, Claim 4 requires that the step of causing the second data processor to send an encryption key to the third data processor is initiated in response to a message from the first data processor to the second data processor. The Examiner states that Chen discloses that the second processor sends a message and key to the first data processor, and cites item 35 in Figure 1A as supporting this assertion.

Item 35 in Figure 1A is the token issuer, i.e., the second data processor of Claim 1. The issue is not whether a message is sent from the token issuer to third data processor containing the encryption key, but rather the event that triggers the transmission. As noted above, the Examiner inherently argues that the authentication server is the first data processor

of Claim 1, the client is the third data processor, and the token issuer is the third data processor. Claim 4 requires that the token issuer sends the public key to the client in response to a message from the authentication server.

Applicant can find no teaching in Chen with respect to the event that causes the distribution of the public key encryptions keys to the clients. Furthermore, Chen teaches that token issuer sends the certificates and keys to the authentication server at the same time or after the token server sends the key to the client. Hence, it would appear that the key is sent in response to a message from some other entity or part of the internal workings of the token server. Accordingly, Applicant submits the Examiner has not satisfied the Examiner's burden of proof with respect to the rejection of Claim 4, and hence, there are additional grounds for allowing Claim 4.

E. Rejection of Claim 5

In addition to the limitations of Claim 1, Claim 5 requires that the network segnent connecting the second and third data processors comprises the internet. The Examiner points to item 5 as comprising the internet in support of the Examiner's assertion that Chen teaches the additional limitation of Claim 5.

As noted above, the second and third data processors identified by the Examiner are the token issuer and the client computer. These computers communicate directly with each other in the scheme shown in Chen. They do not use network 5 identified by the Examiner. Accordingly, there are additional grounds for allowing Claim 5.

F. Rejection of Claim 6

In addition to the limitations of Claim 1, Claim 6 requires that the network segment connecting the first and third data processors comprises a local area network. The Examiner points to the passage at col. 1, lines 50-59 of Chen as teaching this limitation. Once again, Applicant must disagree.

The first and third data processors correspond to the authentication server and the client computer, respectively. These computers communicate with each other over the internet in the scheme shown in Chen.

Furthermore, the passage identified by the Examiner does not refer to any local area network. The passage does mention a firewall. However, firewalls are often implemented on the computer to be protected, and hence, do not require a local area network. Hence, there are additional grounds for allowing Claim 6.

G. Rejection of Claim 7

In addition to the limitations of Claim 1, Claim 7 requires that the network segment connecting the first and third data processors has a higher level of security than the network segment connecting the second and third data processors. The Examiner points to the passage at col. 2, lines 8-18 as teaching this limitation. Once again, Applicant must disagree. The cited passage does not refer to the relative security of the network segments. The passage relates to the increased security provided by the scheme taught in Chen.

As noted above, the first and third data processors of Claim 1 must correspond to the authentication server and client computers, respectively, in the scheme taught in Chen. As noted above, these computers communicate over the internet, the lowest security network segment. The second and third data processors, i.e., the token issuer and client computer, respectively, communicate directly in the scheme taught in Chen. This is the segment having the highest security. Hence, if anything, Chen teaches away from the limitation of Claim 7. Hence, there are additional grounds for allowing Claim 7.

H. Rejection of Claim 8

In addition to the limitations of Claim 1, Claim 8 requires that the first encryption protocol require less computational resources than the second encryption protocol. The Examiner points to the same passages indicated in the Examiner's rejection of Claim 2 discussed above. This passage does not teach anything with respect to the existence or the nature of the first encryption protocol,

As noted above, Chen teaches that the token issuer provide a public key to the client in a message sent from the token issuer to the client. The first encryption protocol of Claim 1 is the protocol used to send this message. However, Chen is silent as to whether or not this message is encrypted. Hence, the Examiner has not satisfied the Examiner's burden of

showing that this message must have been encrypted with a protocol requiring less computational resources than the public key protocol. Accordingly, there are additional grounds for allowing Claim 8.

VII. CONCLUSION

Appellants respectfully submit that for the reasons of fact and law argued herein, the decision of the Examiner in finally rejecting Claims 1-8 should be reversed.

I hereby certify that this paper (along with any others attached hereto) is being sent via facsimile to fax number: 571-273-8300

Respectfully Submitted,

Calvin B. Ward
Registration No. 30,896
Date: July 24, 2006

Agilent Technologies, Inc.
Legal Department, M/S DL429
Intellectual Property Administration
P.O. Box 7599
Loveland, CO 80537-0599
Telephone (925) 855-0413
Telefax (925)855-9214

APPENDIX

THE CLAIMS ON APPEAL:

1. A method for operating a computer system having first, second, and third data processors connected by a network wherein said second and third data processors are connected by an insecure network segment, said method comprising the steps of:

causing said second data processor to send an encryption key for a first encryption protocol to said third data processor utilizing a second encryption protocol;

causing said third data processor to forward said encryption key to said first data processor; and

causing said first data processor to send a message to said second data processor utilizing said encryption key and said first encryption protocol, said message being sent over a communication path comprising said insecure network segment.

2. The method of Claim 1 wherein said first data processor has insufficient computational resources to execute said second encryption protocol.

3. The method of Claim 1 wherein said second encryption protocol is a public key encryption protocol.

4. The method of Claim 1 wherein said step of causing said second data processor to send an encryption key is initiated in response to a message from said first data processor to said second data processor.

5. The method of Claim 1 wherein said insecure network segment comprises the Internet.

6. The method of Claim 1 wherein said network segment connecting said first and third data processors comprises a local area network.

7. The method of Claim 1 wherein said first and third data processors are connected by a network segment that has a higher level of security than said insecure network segment.

8. The method of Claim 1 wherein said first encryption protocol requires less computational resources than said second encryption protocol

Evidence Appendix

none

THIS PAGE BLANK (USPTO)

Related Proceedings Appendix

none